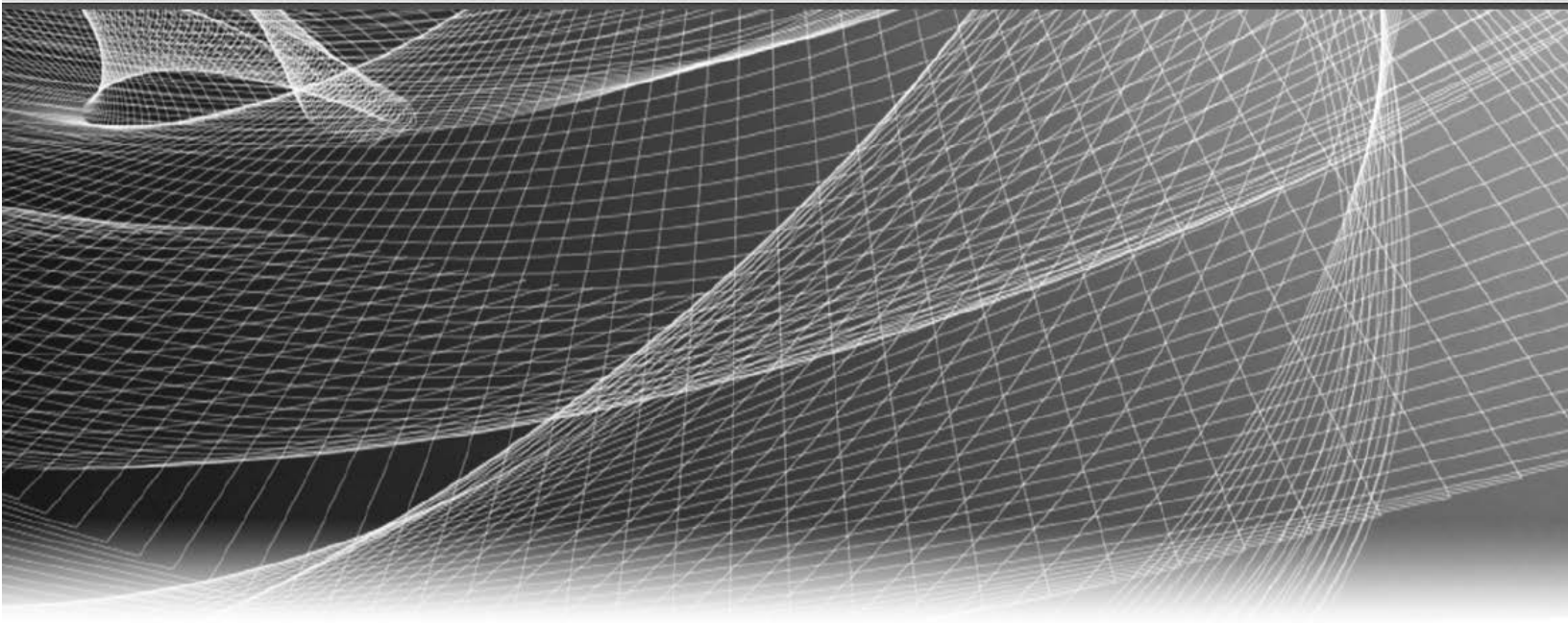

RSA Security Analytics

RSA Archer-Integrationsleitfaden

für Version 10.6

RSA EMC²

Marken

Lizenzvereinbarung

Drittanbieterlizenzen

Hinweis zu Verschlüsselungstechnologien

Verteilung

Inhalt

Integration in RSA Archer

Administratoren können RSA Security Analytics mit RSA Archer Security Operations (SecOps) integrieren, um für das Incident-Management und für Korrekturen Warnmeldungen und Incidents von Security Analytics an Archer zu senden. Dieser Leitfaden enthält einen allgemeinen Workflow zum Konfigurieren dieser Integration.

Durch die Integration von Security Analytics in RSA Archer SecOps erreichen Sie Folgendes:

- Incident Management: Sämtliche in Security Analytics erstellten Incidents können in Archer das komplette Incident-Management durchlaufen.
- Incident-Korrektur: Die Verarbeitung von Incidents erfolgt in Security Analytics, aber Korrekturaufgaben können optional in Archer exportiert werden.

Archer SecOps-Version	Integration in Security Analytics 10.5	Referenz
1.1	Modul ESA (Event Stream Analysis)	Siehe das Thema **Konfigurieren von Vorlagen** im *Systemkonfigurationsleitfaden*: Systemkonfiguration > Standardverfahren > Konfigurieren von Vorlagen für Benachrichtigungen > Konfigurieren von Vorlagen
1.2	Incident Management	Siehe das Thema **Konfigurieren von Integrationseinstellungen zur Verwaltung von Incidents in RSA Archer Security-Operationen** im Leitfaden *Incident Management*: Incident Management > Systemintegration > Konfigurieren von Integrationseinstellungen zur Verwaltung von Incidents in RSA Archer Security-Operationen

Themen

Konfigurieren von Security Analytics für das Arbeiten mit Archer

RSA Security Analytics kann so konfiguriert werden, dass Warnmeldungen und Incidents für das Incident-Management und die Korrektur an RSA Archer gesendet werden. Durch die Integration von Security Analytics in RSA Archer SecOps erreichen Sie Folgendes:

- Incident Management: Sämtliche in Security Analytics erstellten Incidents können in Archer das komplette Incident-Management durchlaufen.
- Incident-Korrektur: Die Verarbeitung von Incidents erfolgt in Security Analytics, aber Korrekturaufgaben können optional in Archer exportiert werden.

Mit der RSA Archer Security Operations Management-Lösung können Sie alle verwertbaren Sicherheitswarnungen zusammenführen. Damit können Sie bei der Reaktion auf Incidents und dem SOC-Management effektiver, proaktiver und zielgerichteter arbeiten. Weitere Informationen zu den RSA Archer SecOps-Funktionen finden Sie in der RSA Archer-Dokumentation in der RSA Archer-Community oder in der RSA Archer Exchange-Community.

Informationen zu den unterstützten Archer-Plattformen finden Sie im *SecOps-Installationshandbuch*.

Die Version von RSA Archer bestimmt, wie RSA Security Analytics integriert wird.

- RSA Archer Security Operations Management 1.2 wird mithilfe von RSA UCF (Unified Collector Framework), das aus einem SAIM-Integrationsservice und RCF (RSA Connector Framework) besteht, in RSA Security Analytics integriert.
- RSA Archer Security Operations Management 1.3 wird mithilfe von RSA UCF (Unified Collector Framework), das aus einem SAIM-Integrationsservice und einem SecOps-Watchdog-Service besteht, in RSA Security Analytics integriert.

Integrationsmethoden

Sie müssen die Systemintegrationseinstellungen konfigurieren, um den Incident-Workflow in RSA Archer Security Operations Management zu managen. Wenn diese Einstellung aktiviert ist, werden Incidents und Korrekturaufgaben nicht mehr in RSA Security Analytics angezeigt.

Informationen zur Konfiguration von Systemintegrationseinstellungen zur Verwaltung von Incident-Workflows in RSA Archer Security Operations finden Sie im Thema **Konfigurieren von Integrationseinstellungen zur Verwaltung von Incidents in RSA Archer Security Operations** im *Leitfaden Incident Management* (Incident Management > Systemintegration > Konfigurieren von Integrationseinstellungen zur Verwaltung von Incidents in RSA Archer Security Operations).

Security Analytics Incident Management Integration Service (SAIM)

Mithilfe von SAIM (Security Analytics Incident Management Integration Service) werden die RSA Archer Security Operations Management-Lösungen 1.2 und 1.3 in das RSA Security Analytics Incident Management-Modul integriert. Sie können eine der folgenden Integrationsoptionen wählen:

- Incident-Workflow ausschließlich in RSA Archer Security Operations Management managen. Bei Auswahl dieser Option werden Incidents durch den Security Analytics Incident Management Integration Service aus dem Security Analytics Incident Management-Modul in die Lösung übermittelt.
- Incident-Workflows im Security Analytics Incident Management-Modul managen und Analysten die Option zum Eskalieren von Korrekturaufgaben und offenen Datenschutzverletzungen für Management und Korrekturen in der RSA Archer Security Operations Management-Lösung ermöglichen. Bei Auswahl dieser Option werden Korrekturaufgaben (als Befunde erstellt) und/oder Datenschutzverletzungen durch den Security Analytics Incident Management Integration Service übermittelt.

Hinweis: Sie müssen in RSA Security Analytics und dem Security Analytics Incident Management Integration Service dieselben Optionen konfigurieren.

RSA Unified Collector Framework

RSA Security Analytics wird mithilfe von RSA UCF (Unified Collector Framework) in RSA Archer SecOps 1.3 integriert.

Das RSA Unified Collector Framework kann in alle unterstützten SIEM-Tools und die RSA Archer Security Operations Management-Lösung integriert werden. Bei der Integration desRSA Security Analytics Incident Management-Moduls können Sie eine der folgenden Integrationsoptionen auswählen:

- Incident-Workflow ausschließlich in RSA Archer Security Operations Management managen. Bei Auswahl dieser Option werden Incidents durch das Unified Collector Framework aus dem Security Analytics Incident Management-Modul in die Lösung übermittelt.

- Incident-Workflows im Security Analytics Incident Management-Modul managen und Analysten die Option zum Eskalieren von Korrekturaufgaben und offenen Datenschutzverletzungen für Management und Korrekturen in der RSA Archer Security Operations Management-Lösung ermöglichen. Wenn Sie diese Option auswählen, übermittelt das Unified Collector Framework Korrekturaufgaben (erstellt als Befunde) und/oder Datenschutzverletzungen.

Hinweis:
• Sie müssen in RSA Security Analytics und dem Unified Collector Framework dieselbe Option konfigurieren.
• Die Integration des RSA Security Analytics Incident-Moduls mit Reporting Engine oder ESA kann zu in RSA Archer SecOps erstellten duplizierten Ereignissen und Incidents führen.

UCF unterstützt mehrere Verbindungen von SIEM-Tools gleichzeitig, z. B. Unterstützung von Security Analytics Reporting Engine, HP ArcSight und Security Analytics Incident Management. Verschiedene Instanzen desselben SIEM-Tools werden jedoch nicht unterstützt, z. B. die gleichzeitige Verbindung von zwei Security Analytics-Servern mit dem gleichen UCF.

Voraussetzungen

- Installieren von RSA Archer Security Operations Management. Siehe RSA Archer-Dokumentation in der RSA Archer-Community oder auf der Registerkarte „Content“ unter https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange.
- Security Analytics 10.5 oder höher ist kompatibel mit SecOps 1.2 und SecOps 1.3. Security Analytics 10.5 ist auch mit SecOps 1.1 kompatibel, dies wird jedoch nicht empfohlen.
- Bei Verwendung von Security Analytics 10.6 wird ein Upgrade auf SecOps 1.3 empfohlen.
- Stellen Sie sicher, dass das Modul Incident Management in RSA Security Analytics konfiguriert ist.
- Zur Verwendung von Archer SecOps 1.3 müssen Sie ein Benutzerkonto für den Webserviceclient erstellen, der zur Übermittlung der Daten an die RSA Archer GRC-Plattform verwendet werden soll.

RSA Unified Collector Framework-Integrationen

Mit dem RSA UCF (Unified Collector Framework) können Sie Ihr RSA Archer Security Operations Management-System in die folgenden Anwendungen integrieren:

- Security Analytics Incident Management (SA IM)
- Security Analytics Reporting Engine (SA RE)
- Security Analytics Event Stream Analysis (SA ESA)

Erstellen von RSA Archer-Benutzerkonten für Push- und Pull

Es sind zwei RSA Archer-Benutzerkonten erforderlich, um Konflikte beim Senden und Empfangen von Daten von RSA Security Analytics zu vermeiden.

1. Klicken Sie auf **Administration** > **Zugriffskontrolle** > **Benutzer managen** > **Neu**.
2. Geben Sie in den Feldern „Vorname“ und „Nachname“ einen Namen ein, der angibt, dass das UCF dieses Konto für den Daten-Push-Vorgang in RSA Archer GRC verwendet. Beispiel: UCF-Benutzer, Push.

   Hinweis: Geben Sie beim Konfigurieren des Pull-Kontos einen Namen ein, der angibt, dass das UCF dieses Konto für Daten-Pull-Vorgänge von RSA Archer GRC verwendet. Beispiel: UCF-Benutzer, Pull.
3. (Optional) Geben Sie einen Benutzernamen für dieses neue Benutzerkonto ein.

   Hinweis: Wenn Sie keinen Benutzernamen angeben, wird der Benutzername von der RSA Archer GRC-Plattform aus dem ersten und letzten Namen erstellt, die eingegeben werden, wenn Sie das neue Benutzerkonto speichern.
4. Geben Sie im Abschnitt „Kontaktinformationen“ in das Feld „E-Mail“ eine E-Mail-Adresse ein, die diesem neuen Benutzerkonto zugeordnet werden soll
5. Ändern Sie im Bereich „Lokalisierung“ die Zeitzone in „Koordinierte Weltzeit (UTC)“.

   Hinweis: Das UCF verwendet UTC-Zeit als Basis für alle zeitbezogenen Berechnungen.
6. Geben Sie im Abschnitt „Kontowartung“ ein neues Passwort für das neue Benutzerkonto ein und bestätigen Sie es.

   Hinweis: Notieren Sie den Benutzernamen und das Passwort für das neue Benutzerkonto, das Sie soeben erstellt haben. Sie müssen diese Anmeldedaten eingeben, wenn Sie das UCF für die Kommunikation mit der RSA Archer GRC-Plattform über den Webserviceclient einrichten.
7. Deaktivieren Sie die Option „Kennwortänderung bei der nächsten Anmeldung erzwingen“.
8. Wählen Sie im Feld „Sicherheitsparameter“ den Sicherheitsparameter aus, den Sie für diesen Benutzer verwenden möchten.

Hinweis: Wenn Sie einen Standardsicherheitsparameter mit einem Passwortänderungsintervall von 90 Tagen zuweisen, müssen Sie auch das im SA IM Integration Service gespeicherte Passwort für das Benutzerkonto alle 90 Tage aktualisieren. Um dies zu vermeiden, können Sie optional einen neuen Sicherheitsparameter für das SA IM Integration Service-Benutzerkonto erstellen und das Passwortänderungsintervall auf den gemäß der Standards Ihres Unternehmens zulässigen Höchstwert festlegen.

9. Klicken Sie auf die Registerkarte **Gruppen** und gehen Sie wie folgt vor:
   a. Klicken Sie im Abschnitt „Gruppen“ auf **Abfrage**.
   b. Erweitern Sie im Fenster „Verfügbare Gruppen“ den Punkt „Gruppen“.
   c. Scrollen Sie nach unten und wählen Sie „SOC: Lösungsadministrator“ und „EM: Schreibgeschützt“ aus.
   d. Klicken Sie auf **OK**.
10. Klicken Sie auf **Anwenden** und anschließend auf **Speichern**.
11. Wenn die Einstellungen für Sprache und Region des RSA Archer GRC-Systems auf einen anderen Wert als „Englisch - US“ festgelegt sind, führen Sie die folgenden Schritte aus:
    a. Öffnen Sie das soeben erstellte Benutzerkonto und wählen Sie im Abschnitt „Lokalisierung“ im Feld „Gebietsschema“ die Option „Englisch (USA)“ aus und klicken Sie auf **Speichern**.
    b. Öffnen Sie auf dem Windows-System, auf dem die RSA Archer GRC-Plattform gehostet wird, den Internetinformationsdienste-Manager (IIS).
    c. Blenden Sie den RSA Archer GRC-Standort ein, klicken Sie auf „.Net Globalisierung“, wählen Sie in den Feldern „Region“ und „UI-Region“ die Option „Englisch (USA)“ aus und klicken Sie auf **Anwenden**.
    d. Starten Sie die RSA Archer GRC-Standort neu.
12. Wiederholen Sie die Schritte 1 bis 11, um ein zweites Benutzerkonto zu erstellen, mit dem das UCF Daten per Pull von RSA Archer GRC abrufen kann.

Konfigurieren von Endpunkten in RSA Unified Collector Framework

Endpunkte stellen die erforderlichen Verbindungsdetails bereit, damit das UCF die RSA Security Analytics- und RSA Archer GRC-Systeme erreichen kann.

Hinweis: Einige Endpunkte sind erforderlich, um verschiedene Integrationen verwenden zu können. Die folgende Liste enthält die obligatorischen Endpunkte.

Obligatorische Endpunkt-Integration

- Archer Push Syslog-Endpunkt
- Security Analytics Incident Management (SA IM)
- Archer Pull Enterprise Management-Plug-in-Endpunkt
- Modusauswahl: SecOps- oder Nicht-SecOps-Modus.
- Syslog-Server
- Enterprise-Management

Hinweis:
• Wenn der Modus „Nicht-SecOps“ aktiviert ist, werden Incidents in SA IM anstelle von RSA Archer Security Operations Management gemanagt.
• Sie müssen die Ports für TCP, sicheres TCP und UDP konfigurieren.
• Stellen Sie sicher, dass der Name des Betreffs des Zertifikats für den RSA Archer GRC-Server dem Hostnamen entspricht.

Verfahren

1. Öffnen Sie den Verbindungsmanager auf dem UCF-System wie folgt:
   a. Öffnen Sie eine Eingabeaufforderung.
   b. Wechseln Sie zum Verzeichnis <*install_dir*>\SA IM integration service\data-collector.
   c. Geben Sie Folgendes ein:

      ```
      runConnectionManager.bat
      ```

2. Geben Sie im Verbindungsmanager **1** für „Endpunkt hinzuzufügen“ ein.
3. Fügen Sie wie folgt einen Endpunkt für Daten-Push-Vorgänge an RSA Archer Security Operations Management hinzu:
   a. Geben Sie die Zahl für Archer ein.

      Hinweis: SSL muss aktiviert sein, um die RSA Archer-Endpunkte hinzufügen zu können.

   b. Geben Sie als Name des Endpunkts **Push** ein.
   c. Geben Sie die URL des RSA Archer GRC-Systems ein.
   d. Geben Sie den Instanznamen des RSA Archer GRC-Systems ein.
   e. Geben Sie den Benutzernamen des Benutzerkontos ein, das Sie erstellt haben, um Daten per Push in das RSA Archer GRC-System zu übertragen.
   f. Geben Sie das Passwort für das Benutzerkonto ein, das Sie erstellt haben, um Daten per Push in das RSA Archer GRC-System zu übertragen, und bestätigen Sie das Passwort.
   g. Wenn Sie gefragt werden, ob dieses Konto für Pull-Vorgänge von Daten verwendet wird, geben Sie **False** ein.
4. Fügen Sie wie folgt einen Endpunkt für das Abrufen von Daten per Pull aus RSA Archer Security Operations Management hinzu:
   a. Geben Sie die Zahl für Archer ein.

      Hinweis: SSL muss aktiviert sein, um die RSA Archer-Endpunkte hinzufügen zu können.

   b. Geben Sie als Name des Endpunkts **Pull** ein.
   c. Geben Sie die URL des RSA Archer GRC-Systems ein.
   d. Geben Sie den Instanznamen des RSA Archer GRC-Systems ein.

e. Geben Sie den Benutzernamen des Benutzerkontos ein, das Sie erstellt haben, um Daten per Pull von dem RSA Archer GRC-System abzurufen.

f. Geben Sie das Passwort für das Benutzerkonto ein, das Sie erstellt haben, um Daten per Pull von dem RSA Archer-System abzurufen, und bestätigen Sie das Passwort.

g. Wenn Sie gefragt werden, ob dieses Konto für Pull-Vorgänge von Daten verwendet wird, geben Sie **True** ein.

5. Fügen Sie wie folgt einen Endpunkt für RSA Security Analytics Incident Management hinzu:

a. Geben Sie die Zahl für Security Analytics IM ein.

b. Geben Sie einen Namen für den Endpunkt ein.

c. Geben Sie die IP-Adresse des SA-Hosts ein.

d. Geben Sie für „SA-Port“ den Wert **5671** ein.

e. Geben Sie die Zielwarteschlange für Korrekturaufgaben ein. Wählen Sie dabei alle Prozesse aus, sowohl „Integration in RSA Archer“ als auch „IT-Helpdesk (Vorgänge)“.

f. Gehen Sie wie folgt vor, um automatisch Zertifikate zum Security Analytics-Truststore hinzuzufügen:

i. Geben Sie **Ja** ein.

ii. Geben Sie den Hostnamen, den Benutzernamen und das Passwort für SA ein.

Hinweis: Wenn ein Fehler angezeigt wird, dass der Zertifizierungsstellen-Truststore nicht festgelegt werden konnte, lesen Sie die Informationen unter Troubleshooting einer RSA Archer-Integration.

6. Wählen Sie im UCF-Verbindungsmanager wie folgt den Modus:

a. Geben Sie die Zahl für „Modusauswahl“ ein.

b. Wählen Sie eine der folgenden Optionen:

- Incident-Workflow in RSA Security Analytics managen
- Incident-Workflow ausschließlich in RSA Archer Security Operations Management managen

7. Fügen Sie zum Verwenden von Integrationen von Drittanbietern den Syslog-Serverendpunkt wie folgt hinzu:

a. Geben Sie die Zahl für „Syslog-Serverendpunkt“ ein.

b. Geben Sie Folgendes ein:

- Feldbeschreibung
- SSL konfiguriert
- TCP-Port
- Sicherer TCP-Port, wenn der Syslog-Client die Syslog-Meldung im sicheren TCP-Modus sendet.

Hinweis: Der Standardwert ist 1515. Wenn Sie den Syslog-Server in diesem Modus nicht hosten möchten, geben Sie **0** ein.

TCP-Port: Geben Sie den TCP-Port ein, wenn der Syslog-Client die Syslog-Meldung im TCP-Modus sendet.

Hinweis: Der Standardwert ist 1514. Wenn Sie den Syslog-Server in diesem Modus nicht hosten möchten, geben Sie **0** ein.

UDP-Port: Geben Sie den UDP-Port ein, wenn der Syslog-Client die Syslog-Meldung im UDP-Modus sendet.

Hinweis: Der Standardwert ist 514. Wenn Sie den Syslog-Server in diesem Modus nicht hosten möchten, geben Sie **0** ein.

Standardmäßig wird der Syslog-Server in den oben genannten drei Modi ausgeführt, es sei denn, er wird durch Eingabe von 0 deaktiviert.

8. Geben Sie zum Testen des Syslog-Clients die Zahl für „Syslog-Client testen“ ein. Verwenden Sie „Syslog-Client testen“ mit den Dateien aus <*install_dir*>\SA IM integration service\config\mapping\test-files\.
9. Geben Sie im Verbindungsmanager **5** ein, um jeden Endpunkt zu testen.

Konfigurieren der Syslog-Ausgabeaktion für die Reporting Engine für Security Analytics 10.5

Hinweis: Dieses Verfahren bezieht sich auf SecOps 1.3 mit Security Analytics 10.5.

1. Navigieren Sie in Security Analytics zu **Administration** > **Services**.
2. Wählen Sie den Reporting Engine-Service aus und klicken Sie auf **System** > **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Ausgabeaktionen**.

4. Geben Sie im Bereich „SA-Konfiguration“ in das Feld „Hostname“ den Hostnamen oder die IP-Adresse des Reporting Engine-Servers ein.

   Hinweis: Wenn Sie in diesem Feld keinen Wert eingeben, funktioniert die Verbindung zu Security Analytics in der RSA Archer Security Alerts-Anwendung nicht.

5. Fügen Sie die Syslog-Konfiguration wie folgt hinzu:

   a. Geben Sie im Feld „Servername“ den Hostnamen des UCF ein

   b. Geben Sie im Feld „Serverport“ den Port ein, den Sie in der UCF-Syslog-Konfiguration ausgewählt haben.

   c. Wählen Sie im Feld „Protokoll“ das Transportprotokoll aus.

   Hinweis: Wenn Sie „Sicheres TCP“ auswählen, muss SSL konfiguriert werden.

6. Klicken Sie auf **Speichern**.

Konfigurieren von ESA-Syslog-Benachrichtigungseinstellungen in Security Analytics 10.5 oder höher

Dieses Verfahren bezieht sich auf SecOps 1.3 mit Security Analytics 10.5 oder höher.

1. Klicken Sie auf **Administration** > **System** > **Globale Benachrichtigungen**.
2. Klicken Sie auf die Registerkarte **Ausgabe**.
3. Definieren und aktivieren Sie eine ESA-Syslog-Benachrichtigung.
4. Klicken Sie auf die Registerkarte **Server**.
5. Definieren und aktivieren Sie einen Syslog-Benachrichtigungsserver.
6. Geben Sie im Bereich „Syslog-Serverkonfiguration“ Folgendes ein:

Feld	Beschreibung
Servername	Geben Sie den Hostnamen oder die IP-Adresse des Systems an, auf dem Sie das UCF installiert haben.
Serverport	Geben Sie die Portnummer an, die das UCF für die Erfassung von Syslog-Warnmeldungen verwenden soll.
Facility	Geben Sie die Syslog-Facility an.
Protokoll	Wählen Sie das Protokoll aus.

7. Klicken Sie auf **Speichern**.

Konfigurieren von Incident Management für die Integration in Archer SecOps 1.3

Gehen Sie in Security Analytics wie folgt vor, um Incident Management für Archer SecOps 1.3 zu konfigurieren:

Aufgabe/Link zu Anweisungen
Schritt 1: Konfigurieren der Incident Management-Datenbank
Schritt 2: Auswählen des Modus für Security Analytics Incident Management
Schritt 3: Konfigurieren der Weiterleitung an den Security Analytics Incident Management Service
Schritt 4: Weiterleiten von ECAT-Warnmeldungen an den Security Analytics Incident Management Service
Schritt 5: Aggregieren von Warnmeldungen zu Incidents

Schritt 1: Konfigurieren der Incident Management-Datenbank

Sie müssen die Datenbank für den Incident Management-Service konfigurieren, damit sie verwendet werden kann.

So konfigurieren Sie eine Datenbank für den Incident Management-Service:

1. Wählen Sie im Menü **Security Analytics** die Optionen >Administration **Services** aus.

   Die Ansicht Services wird angezeigt.

2. Wählen Sie im Bereich „Services“ den Incident Management-Service und  **> Ansicht > Durchsuchen** aus.

   Die Serviceübersicht wird angezeigt.

3. Wählen Sie im Bereich „Optionen“ die Optionen **Service > Konfiguration > Datenbank** aus.

   Die Datenbankansicht wird im rechten Bereich angezeigt.

4. Stellen Sie folgende Informationen bereit:

   - Host: Der Hostname oder die IP-Adresse des ESA-Hosts, der als Datenbank ausgewählt wurde
   - DatabaseName: im (Standardwert)

- Port: 27017 (Standardwert)
- Benutzername: Der Benutzername für das Benutzerkonto der IM-Datenbank (ESA erstellt einen IM-Benutzer mit den entsprechenden Berechtigungen.)
- Passwort: Das für den IM-Benutzer ausgewählte Passwort

5. Starten Sie den Incident Management-Service mit dem folgenden Befehl neu:

```
service rsa-im restart
```

Hinweis: Der Neustart des Incident Management-Services ist wichtig, damit die Datenbankkonfiguration abgeschlossen werden kann.

Schritt 2: Auswählen des Modus für Security Analytics Incident Management

So wählen Sie die Workflowmanagementmethode in Security Analytics aus:

1. Klicken Sie im Menü **Security Analytics** auf >Incidents **Konfigurieren**.
2. Klicken Sie auf die Registerkarte **Integration**.
3. Wählen Sie eine der folgenden Optionen:
   - Incident-Workflow in RSA Security Analytics managen
     - Ermöglicht Analysten, Korrekturaufgaben für die Zielwarteschlange **Operationen** als Tickets zu eskalieren.
     - Ermöglicht Analysten, Korrekturaufgaben für die Zielwarteschlange **GRC** als Befunde zu eskalieren.
     - Ermöglicht Analysten, Datenschutzverletzungen zu melden und den Prozess zur Behandlung von Datenschutzverletzungen in der Lösung RSA Archer Security Operations Management auszulösen.

       Weitere Informationen finden Sie unter **Konfigurieren von Integrationseinstellungen zur Verwaltung von Incidents in Security Analytics** im Leitfaden *Incident Management*.
   - Incident-Workflow ausschließlich in RSA Archer Security Operations Management managen
4. Klicken Sie auf **Anwenden**.

Hinweis: Dieser Schritt gilt auch für die Integration in Archer SecOps 1.2.

Schritt 3: Konfigurieren der Weiterleitung an den Security Analytics Incident Management Service

- Gehen Sie wie folgt vor, um Security Analytics Event Stream Analysis-Warnmeldungen an Security Analytics Incident Management weiterzuleiten:
  a. Wählen Sie im Menü „Security Analytics“ die Optionen **Administration > Services > ESA-Service** aus.
  b. Wählen Sie einen ESA-Service und dann  **> Ansicht > Konfiguration** aus.
  c. Klicken Sie auf die Registerkarte **Advanced**.
  d. Vergewissern Sie sich, dass das Kontrollkästchen „Warnmeldungen an Nachrichtenbus weiterleiten“ standardmäßig ausgewählt ist. Aktivieren Sie, falls erforderlich, das Kontrollkästchen **Warnmeldungen an Nachrichtenbus weiterleiten** und klicken Sie auf **Anwenden**.
- Gehen Sie wie folgt vor, um Warnmeldungen der Security Analytics Reporting Engine an Security Analytics Incident Management weiterzuleiten:
  a. Klicken Sie in Security Analytics auf **Administration > Services > Reporting Engine-Service**.
  b. Klicken Sie für den Reporting Engine-Service auf  **> Ansicht > Konfiguration**.
  c. Klicken Sie auf die Registerkarte **Allgemein**.
  d. Aktivieren Sie im Abschnitt **Systemkonfiguration** das Kontrollkästchen **Warnmeldungen an IM weiterleiten** und klicken Sie auf **Anwenden**.
- Gehen Sie wie folgt vor, um Security Analytics Malware Analysis-Warnmeldungen an Security Analytics Incident Management weiterzuleiten:
  a. Klicken Sie in Security Analytics auf **Administration > Services > Malware Analysis-Service**.
  b. Klicken Sie für den MA-Service auf  > **Ansicht** > **Konfiguration**.
  c. Klicken Sie auf die Registerkarte **Auditing**.
  d. Überprüfen Sie im Abschnitt „Incident Management Alerting“, ob das Kontrollkästchen **Aktivierter Konfigurationswert** aktiviert ist. Wenn das Kontrollkästchen nicht aktiviert ist, aktivieren Sie es und klicken Sie auf **Anwenden**.

Schritt 4: Weiterleiten von ECAT-Warnmeldungen an den Security Analytics Incident Management Service

RSA ECAT-Warnmeldungen können über Security Analytics Incident Management an RSA Archer GRC gesendet werden.

1. Konfigurieren Sie „Warnmeldungen über den Nachrichtenbus“: *Konfigurieren von ECAT-Warnmeldungen über Nachrichtenbus*.
2. Klicken Sie in RSA ECAT auf **Konfiguration > Überwachung und externe Komponenten**.
3. Wählen Sie im Fenster „Konfiguration externer Komponenten“ den Incident Message Broker aus.
4. Klicken Sie auf „Hinzufügen“ (+).
5. Füllen Sie die folgenden Felder aus:
   - Instanzenname
   - Hostname/IP des Servers Geben Sie die Host-DNS- oder IP-Adresse des RSA Security Analytics-Servers ein.
   - Portnummer: Der Standardport ist 5671.
6. Klicken Sie auf **Speichern**.

Schritt 5: Aggregieren von Warnmeldungen zu Incidents

In Security Analytics Incident Management eingehende Warnmeldungen können automatisch zu Incidents aggregiert und an RSA Archer Security Operations Management weitergeleitet werden. Aggregationsregeln werden automatisch jede Minute ausgeführt und aggregieren die Warnmeldungen basierend auf den ausgewählten Übereinstimmungsbedingungen und Gruppierungsoptionen zu Incidents. Weitere Informationen zur Aggregation von Warnmeldungen finden Sie im Thema **Konfigurieren von Warnmeldungsquellen zur Anzeige von Warnmeldungen in Incident Management** im *Konfigurationsleitfaden für Incident Management*.

So konfigurieren Sie die Aggregation von Warnmeldungen:

1. Navigieren Sie in Security Analytics zu **Incidents > Konfiguration > Aggregationsregeln**.
2. Gehen Sie wie folgt vor, um die bereitgestellten einsatzbereiten Regeln zu aktivieren:
   a. Doppelklicken Sie auf die Regel.
   b. Wählen Sie **Aktiviert** aus.

c. Klicken Sie auf **Speichern**.

d. Wiederholen Sie die Schritte a bis c für jede Regel.

3. Gehen Sie wie folgt vor, um eine neue Regel hinzuzufügen:

a. Klicken Sie auf „Hinzufügen“ (+).

b. Wählen Sie **Aktiviert** aus.

c. Füllen Sie die folgenden Felder aus:

- Regelname
- Aktion
- Bedingungen abstimmen
- Gruppierungsoptionen
- Incident-Optionen
- Priorität
- Benachrichtigungen

4. Klicken Sie auf **Speichern**.

Konfigurieren der Syslog-Ausgabeaktion für die Reporting Engine für Security Analytics

1. Navigieren Sie in Security Analytics zu **Administration > Services**.
2. Wählen Sie den Reporting Engine-Service aus und klicken Sie auf „System > Konfiguration“.
3. Klicken Sie auf die Registerkarte **Ausgabeaktionen**.
4. Geben Sie im Bereich „SA-Konfiguration“ in das Feld „Hostname“ den Hostnamen oder die IP-Adresse des Reporting Engine-Servers ein.
5. Fügen Sie die Syslog-Konfiguration wie folgt hinzu:

a. Geben Sie im Feld „Servername“ den Hostnamen des UCF ein.

b. Geben Sie im Feld „Serverport“ den Port ein, den Sie in der UCF-Syslog-Konfiguration ausgewählt haben.

c. Wählen Sie im Feld „Protokoll“ das Transportprotokoll aus.

Hinweis: Wenn Sie „Sicheres TCP“ auswählen, muss SSL konfiguriert werden.

6. Klicken Sie auf **Speichern**.

Konfigurieren von SA RE-SSL für sichere Syslog-Server

Konfigurieren Sie SSL, wenn der Syslog-Server mit „Sicheres TCP“ konfiguriert ist.

1. Kopieren Sie das Zertifikat keystore.crt.der von <*install_dir*>\RSA\SA IM integration service\cert-tool\certs auf dem UCF-Computer nach **/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.65-0.b17.el6_7.x86_64/jre/lib/security** auf dem Security Analytics-Server.
2. Führen Sie den folgenden Befehl aus:

```
keytool -import -file keystore.crt.der -alias ucf-syslog -
keystore cacerts -storepass changeit
```

Hinweis: Verwenden Sie nicht Kopieren und Einfügen, um den obigen Befehl einzugeben. Geben Sie ihn zur Vermeidung von Fehlern manuell ein.

3. Legen Sie **ServerCertificateValidationEnabled** auf **true** fest.
   - Navigieren Sie zur Seite „Administration“ der SA-Benutzeroberfläche.
   - Klicken Sie auf **Ansicht > Durchsuchen** des Reporting Engine-Services.
   - Erweitern Sie com.rsa.soc.re.
   - Erweitern Sie sslContextConfiguration und legen Sie für ServerCertificateValidationEnabled **true** fest.
4. Starten Sie den RE-Service neu.

Konfigurieren von Regeln in Security Analytics

1. Klicken Sie auf **Berichte > Managen**.
2. Klicken Sie unter „Gruppen“ auf **Regeln**.
3. Klicken Sie auf „Hinzufügen“ (+).
4. Geben Sie für die neue Gruppe einen Namen ein.
5. Wählen Sie die erstellte Gruppe aus und klicken Sie in der Symbolleiste „Regel“ auf **Hinzufügen (+)**.

6. Geben Sie im Feld „Syslog-Name“ einen Namen für die SecOps-Syslog-Konfiguration ein, die zum Konfigurieren von Warnmeldungen verwendet werden soll.
7. Wählen Sie im Feld „Regeltyp“ die Option „NetWitness-DB“ aus.
8. Geben Sie einen Namen für die Regel ein.
9. Geben Sie in den Feldern „Auswählen“ und „Wobei“ der zu erstellenden Regel entsprechende Werte ein.

   Hinweis: Fügen Sie die Syslog-Konfiguration mit dem oben festgelegten Syslog-Namen hinzu.

10. Klicken Sie auf **Save**.

Hinweis: Um zu erreichen, dass in SA RE und RSA Archer GRC dieselbe Anzahl von Warnmeldungen angezeigt wird, vergewissern Sie sich, dass Sie auf den Registerkarten „Syslog“ und „Datensatz“ für die Ausführung jeweils „Einmal“ ausgewählt haben.

Hinzufügen von Warnmeldungsvorlagen für die Reporting Engine in Security Analytics

Im Lieferumfang der UCF-Syslog-Konfiguration sind einsatzbereite Warnmeldungsvorlagen enthalten, die Sie beim Erstellen einer Warnmeldung mit einer Syslog-Ausgabeaktion verwenden können. In diesen Vorlagen werden die Kriterien definiert, die in der RSA Archer GRC-Plattform zur Aggregation von Warnmeldungen zu Incidents verwendet werden.

Die Beispielvorlagen befinden sich an folgender Stelle auf dem UCF-System:

<*install_dir*>\SA IM integration service\config\mapping\templates\SecOps_SA_Templates

1. Klicken Sie auf **Berichte > Managen > Warnmeldungen**.
2. Klicken Sie auf die Registerkarte **Vorlage**.
3. Klicken Sie auf „Hinzufügen“ (+).
4. Geben Sie im Feld „Name“ einen Namen für die Vorlage ein.
5. Geben Sie im Feld „Meldung“ die Warnmeldung ein.
6. Klicken Sie auf **Create**.
7. Wiederholen Sie die Schritte 3 bis 6 für jede Warnmeldungsvorlage, die Sie hinzufügen möchten.

Konfigurieren von Warnmeldungen in Security Analytics

In der RSA Security Analytics Reporting Engine ist eine Warnmeldung eine Regel, für die Sie eine kontinuierliche Ausführung planen können und deren Befunde in mehreren verschiedenen Warnmeldungsausgaben protokolliert werden können.

1. Klicken Sie auf **Berichte > Managen > Warnmeldungen**.
2. Klicken Sie auf „Hinzufügen“ (+).
3. Wählen Sie **Aktivieren** aus.
4. Wählen Sie die Regel aus, die Sie erstellt haben.
5. Wählen Sie **Per Push an die Decoder übertragen** aus.

   Hinweis: Wenn Sie in diesem Feld keinen Wert eingeben, funktioniert die Verbindung zu RSA Security Analytics in der RSA Archer Security Alerts-Anwendung nicht.
6. Wählen Sie in der Liste „Datenquellen“ eine Datenquelle aus.
7. Wählen Sie im Abschnitt „Benachrichtigung“ die Option **Syslog** aus.
8. Klicken Sie auf „Hinzufügen“ (+).
9. Füllen Sie die Felder für die Syslog-Konfiguration aus.
10. Wählen Sie im Feld „Textkörpervorlage“ die Vorlage aus, die Sie für diese Syslog-Benachrichtigung verwenden möchten.
11. Klicken Sie auf **Speichern**.

Konfigurieren von ESA-Syslog-Benachrichtigungseinstellungen in Security Analytics

1. Klicken Sie auf **Administration** > **System** > **Globale Benachrichtigungen**.
2. Klicken Sie auf die Registerkarte **Ausgabe**.
3. Definieren und aktivieren Sie eine ESA-Syslog-Benachrichtigung.
4. Klicken Sie auf die Registerkarte **Server**.
5. Definieren und aktivieren Sie einen Syslog-Benachrichtigungsserver.
6. Geben Sie im Bereich „Syslog-Serverkonfiguration“ Folgendes ein:

   Feldbeschreibung:

- Server
- Name
- Geben Sie den Hostnamen oder die IP-Adresse des Systems an, auf dem Sie das UCF installiert haben.
- Server
- Port
- Geben Sie die Portnummer an, die das UCF für die Erfassung von
- Syslog-Warnmeldungen verwenden soll.

Gerät:

- Geben Sie Syslog-Facility fest an.

Protokoll:

- Wählen Sie das Protokoll aus.

7. Klicken Sie auf **Speichern**.

Konfigurieren von SA ESA-SSL für sichere Syslog-Server in Security Analytics

Konfigurieren Sie SSL, wenn der Syslog-Server mit „Sicheres TCP“ konfiguriert ist.

1. Navigieren Sie zu **Administration > Services**.
2. Wählen Sie den ESA-Service aus. Navigieren Sie zu **Durchsuchen > Konfiguration > SSL**.
3. Legen Sie für ServerCertificateValidationEnabled **true** fest.
4. Kopieren Sie das Zertifikat keystore.crt.der von <*install_dir*>\SAIM integration service\cert-tool\certs auf dem UCF-Computer nach **/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.65.0.b17.el6_7.x86_64/jre/lib/security** auf der ESA-Box.
5. Führen Sie den folgenden Befehl aus:

```
keytool -import -file keystore.crt.der -alias ucf-syslog -keystore cacerts -
storepass changeit
```

> **Hinweis:** Verwenden Sie nicht Kopieren und Einfügen, um den obigen Befehl einzugeben. Geben Sie ihn zur Vermeidung von Fehlern manuell ein.

6. Starten Sie den ESA-Service neu.

Hinzufügen von ESA-Warnmeldungsvorlagen in Security Analytics

Im Lieferumfang der UCF-Syslog-Konfiguration sind einsatzbereite Warnmeldungsvorlagen enthalten, die Sie beim Erstellen einer Warnmeldung mit einer Syslog-Ausgabeaktion verwenden können. In diesen Vorlagen werden die Kriterien definiert, die in der RSA Archer GRC-Plattform zur Aggregation von Warnmeldungen zu Incidents verwendet werden.

Die Beispielvorlagen befinden sich an folgender Stelle auf dem UCF-System:

<*install_dir*>\SA IM integration service\config\mapping\templates\SecOps_SA_

Templates\SecOps_SA_ESA_templates.txt

Verfahren:

1. Wählen Sie **Administration > System > Globale Benachrichtigungen** aus.
2. Klicken Sie auf die Registerkarte **Vorlagen**.
3. Klicken Sie auf „Hinzufügen“ (+).
4. Wählen Sie im Feld „Vorlagentyp“ die Option „Event Stream Analysis“ aus.
5. Geben Sie im Feld „Name“ den Namen für die Vorlage ein.
6. (Optional) Geben Sie im Feld „Beschreibung“ eine kurze Beschreibung der Vorlage ein.
7. Geben Sie im Feld „Vorlage“ die Warnmeldung ein.
8. Klicken Sie auf **Speichern**.
9. Wiederholen Sie die Schritte 3 bis 8 für jede Warnmeldungsvorlage, die Sie hinzufügen möchten.

Erstellen von ESA-Regeln in Security Analytics

1. Klicken Sie auf **Warnmeldungen** > **Konfigurieren**.
2. Wählen Sie das ESA-Gerät aus.
3. Klicken Sie auf **Auswählen**.
4. Klicken Sie in der Symbolleiste „ESA-Regeln“ auf +.
5. Wählen Sie „Regelerstellung“ aus.
6. Geben Sie im Feld Name einen Namen für die Regel ein.
7. Geben Sie in das Feld Beschreibung eine Beschreibung für die Regel ein.
8. Wählen Sie einen Schweregrad aus.
9. Gehen Sie im Bereich „Bedingung“ wie folgt vor:

a. Klicken Sie auf +, um eine Anweisung zu erstellen.

b. Geben Sie einen Namen ein und fügen Sie Metadaten/Wertepaare für die Anweisung hinzu.

c. Klicken Sie auf **Save**.

d. Wiederholen Sie die Schritte a bis c, bis Sie alle Ihre Anweisungen für die Regel erstellt haben.

10. Wählen Sie im Abschnitt „Benachrichtigungen“ die Option **Syslog** aus.
11. Wählen Sie die Benachrichtigung, den Syslog-Server und die Vorlage aus, die Sie zuvor erstellt haben.
12. Klicken Sie auf **Speichern** und **Schließen**.
13. Klicken Sie auf **Warnmeldungen** > **Konfigurieren** > **Bereitstellungen**.
14. Klicken Sie für den Bereich „ESA-Services“ auf +.
15. Wählen Sie den ESA-Service aus.
16. Klicken Sie auf **Jetzt bereitstellen**.
17. Klicken Sie im Abschnitt „ESA-Regeln“ auf +, um die erstellte ESA-Regel auszuwählen, und klicken Sie dann auf **Jetzt bereitstellen**.

RSA Archer-Feed

Standardmäßig werden nur die Felder „IP-Adresse“ und „Wichtigkeitsrating“ in der Anwendung RSA Archer Devices durch den Security Analytics Incident Management Integration Service in RSA Security Analytics eingespeist. Sie können das Enterprise-Management-Plug-in so anpassen, dass die Felder „Geschäftsbereich“ und „Facility“, auf die verwiesen wird, in der Anwendung Devices in den Feed einbezogen werden. Weitere Informationen finden Sie in der Archer-Dokumentation unter https://community.emc.com/community/connect/grc_ecosystem/rsa archer oder https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_ exchange.

Hinweis: Wenn Sie vorhaben, die Informationen in „Geschäftsbereich“ und „Facility“ aus der RSA Archer GRC-Plattform per Feed in Live zu übertragen, müssen Sie in der Datei index-concentrator-custom.xml Schlüssel für diese Felder hinzufügen.

Der Administrator kann in Security Analytics mehrere Aufgaben durchführen, darunter die folgenden:

Aufgabe
Aktualisieren von Concentrator- und Decoder-Services
Hinzufügen des RSA Archer Enterprise Management-Endpunkts im UCF
Aktualisieren Sie der RSA Security Analytics-Hostdatei für SSL-Modus
Erstellen einer wiederkehrenden Feedaufgabe

Aktualisieren von Concentrator- und Decoder-Services

Der Security Analytics Incident Management Integration Service managt die Dateien für einen benutzerdefinierten Feed und legt diese Dateien in einem lokalen Ordner ab, den Sie bei der Konfiguration des Security Analytics Incident Management Integration Service angeben. Das Modul Live von RSA Security Analytics ruft die Feeddateien aus diesem Ordner ab. Live überträgt den Datenfeed dann per Push an die Decoder, die basierend auf dem erfassten Netzwerkdatenverkehr und der Feeddefinition mit der Erstellung von Metadaten beginnen. Damit jeder Concentrator die neuen von den Decodern erstellten Metadaten erkennt, müssen Sie die Dateien index-concentrator-custom.xml, index-logdecoder-custom.xml und index-decoder-custom.xml bearbeiten.

1. Klicken Sie im Menü „Security Analytics“ auf **Administration > Services**.
2. Wählen Sie den Concentrator und dann  > **Ansicht > Konfiguration** aus.
3. Klicken Sie auf die Registerkarte **Dateien**.
4. Wählen Sie in der Drop-down-Liste die Datei index-concentrator-custom.xml aus. Führen Sie einen der folgenden Schritte aus:
   - Wenn in der Datei bereits Inhalte vorhanden sind, fügen Sie wie folgt einen Schlüssel für das neue Metadatenelement hinzu:

     ```
     <key description="Criticality" format="Text"
     level="IndexValues"

     name="criticality" defaultAction="Open"/>
     ```

     Hinweis: Verwenden Sie nicht Kopieren und Einfügen, um den obigen Befehl einzugeben. Geben Sie ihn zur Vermeidung von Fehlern manuell ein.
   - Wenn die Datei leer ist, fügen Sie den folgenden Inhalt hinzu:

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
<key description="Criticality" format="Text" level="IndexValues"
name="criticality" defaultAction="Open"/>
</language>
```

5. Klicken Sie auf **Anwenden**.
6. Wenn keine Services aufgeführt sind, klicken Sie auf **Anwenden**.
7. Gehen Sie wie folgt vor, um mehrere Geräte hinzuzufügen:
   a. Klicken Sie auf **Push**.
   b. Wählen Sie die Geräte aus, zu denen Sie diese Datei per Push übertragen möchten.
   c. Klicken Sie auf **OK**.
8. Wiederholen Sie die Schritte 1 bis 7 für die Log Decoder und Index-Decoder mit den Dateien index-logdecoder-custom.xml und index-decoder-custom.xml.
9. Beenden und starten Sie die Concentrator- und Decoder-Services.

Hinzufügen des RSA Archer Enterprise Management-Endpunkts im UCF

1. Wählen Sie im UCF-Verbindungsmanager wie folgt den Modus:
   a. Geben Sie die Zahl für „Modusauswahl“ ein.
   b. Wählen Sie eine der folgenden Optionen:
      - Incident-Workflow in RSA Security Analytics managen
      - Incident-Workflow ausschließlich in RSA Archer Security Operations Management managen
2. Fügen Sie den RSA Archer Enterprise Management-Endpunkt wie folgt hinzu:
   a. Geben Sie die Zahl für Enterprise Management ein.
   b. Füllen Sie die Felder in der Tabelle unten aus.

Feld	Beschreibung
Endpunktname	Optionaler Name des Endpunkts
Webserver-Port	Der Standardwert ist 9090. Kann für das Hosten der Webserver-URL konfiguriert werden. Die URL mit der Portnummer sollte als die URL im SA Live-Feed bereitgestellt werden: http (s)://hostname:port/archer/sa/feed

Feld	Beschreibung
Bedeutung	Wichtigkeit der Ressourcen, die von RSA Archer GRC abgerufen werden sollen. Bei **false** werden Ressourcen mit beliebigem Wichtigkeitsrating abgerufen. Bei **true** werden nur Ressourcen mit hohem Wichtigkeitsrating abgerufen. Bearbeiten Sie zum manuellen Konfigurieren die Eigenschaft „em.criticality“ in der Eigenschaftendatei collector-properties, um eine durch Kommas getrennte Liste von Wichtigkeitsratings bereitzustellen: NIEDRIG, MITTEL, HOCH.
Feedverzeichnis	Verzeichnis, in dem die Ressourcen-CSV-Datei von RSA Archer GRC gespeichert ist. **Hinweis:** Der angegebene Verzeichnispfad muss vorhanden sein.
Webserver-Benutzername	Benutzername für die Authentifizierung auf dem EM-Webserver. **Hinweis:** Dieser wird bei der Konfiguration des SA Live-Feeds angegeben.
Webserverpasswort	Passwort für die Authentifizierung auf dem EM-Webserver. **Hinweis:** Dieser wird bei der Konfiguration des SA Live-Feeds angegeben.
SSL-Modus	Der Standardwert ist „Nein“. Bei **Nein** wird in der URL der HTTP-Modus verwendet: http://hostname:port/archer/sa/feed Bei **Ja** wird in der URL der HTTPS-Modus verwendet: https://hostname:port/archer/sa/feed Wenn Sie die Hostdatei nicht aktualisiert haben, lesen Sie die Informationen unter Aktualisieren Sie der RSA Security Analytics-Hostdatei für SSL-Modus.

3. Wenn Sie für den SSL-Modus „Ja“ ausgewählt haben, füllen Sie die folgenden Felder aus:
   - Zertifikate in die SA-Box kopieren. Geben Sie **Ja** ein, um anzugeben, dass die Zertifikate automatisch von RSA Archer Security Operations Management in RSA Security

Analytics kopiert werden sollen.

- SA-Host Geben Sie den Hostnamen oder die IP-Adresse für den SA-Server an.
- SA-Hostbenutzername. Geben Sie den Benutzernamen für die Anmeldung beim SA-Server zum Kopieren der Zertifikate an.
- SA-Hostpasswort Geben Sie das Passwort für die Anmeldung beim SA-Server zum Kopieren der Zertifikate an.

Hinweis: Wenn das Kopieren der Zertifikate und das Hinzufügen des Endpunkts fehlschlagen, kopieren Sie die Zertifikate manuell. Weitere Informationen finden Sie unter **Manuelles Kopieren von Enterprise Management-Zertifikaten** in Troubleshooting einer RSA Archer-Integration. Nach dem Kopieren der Zertifikate müssen Sie das Enterprise Management-Plug-In hinzufügen, ohne die Zertifikate automatisch zu kopieren.

Aktualisieren Sie der RSA Security Analytics-Hostdatei für SSL-Modus

1. Bearbeiten Sie die Hostdatei auf dem SA-Server am folgenden Speicherort: vi/etc/hosts
2. Geben Sie Folgendes als UCF-Host-IP-Adresse ein:

   ```
   <ucf-host-ip> <ucf-host-name>
   ```

3. Starten Sie den SA-Server durch Ausführen des folgenden Befehls neu:

   ```
   restart jettysrv
   ```

4. Geben Sie bei der Konfiguration des SA Live-Feeds den Hostnamen für die URL statt der in Enterprise Management im UCF konfigurierten IP-Adresse und Portnummer ein:

   ```
   https: //<ucf-host-name> : <EM_Port>/archer/sa/feed.
   ```

5. Überprüfen Sie, ob die Verbindung funktioniert.

Erstellen einer wiederkehrenden Feedaufgabe

Damit RSA Security Analytics Feeddateien aus dem Security Analytics Incident Management Integration Service herunterladen und per Push auf Decoders übertragen kann, müssen Sie eine wiederkehrende Feedaufgabe erstellen und die Datenfeedeinstellungen definieren.

Hinweis: Für RSA Archer SecOps 1.2: Damit RSA Security Analytics Feeddateien von dem RCF-Computer herunterladen und per Push auf Decoder übertragen kann, müssen Sie eine wiederkehrende Feedaufgabe erstellen und die Datenfeedeinstellungen definieren. Das Verfahren ist mit wenigen Ausnahmen dasselbe wie für RSA Archer SecOps 1.3. Weitere Informationen erhalten Sie in der Dokumentation in der RSA Archer Exchange-Community.

1. Klicken Sie im Menü „Security Analytics“ auf **Live > Feeds**.
2. Klicken Sie auf +.
3. Wählen Sie **Benutzerdefinierter Feed** aus und klicken Sie dann auf **Weiter**.
4. Wählen Sie **Wiederkehrend** aus.
5. Geben Sie einen Namen für den Feed ein.
6. Geben Sie im Feld „URL“ eine der folgenden URLs ein:
   - http://ucf_hostname/archer/sa/feed
   - https://ucf_hostname_or_ip:port/archer/sa/feed

   wobei *http(s):ucf_hostname_or_ip:port* die Adresse des SecurityAnalytics Incident Management Integration Service-Systems ist. Verwenden Sie HTTPS, wenn Sie die SSL-Kommunikation mit RSA Security Analytics aktiviert haben. Beispiel: http://10.10.10.10:9090 oder https://10.10.10.10:8443.

   Hinweis: Wenn Incident Management im SSL-Modus ausgeführt wird, muss der Hostname in der URL verwendet werden.
7. Wählen Sie **Authentifiziert**.
8. Geben Sie in die Felder „Benutzername“ und „Passwort“ die Anmeldedaten des Benutzerkontos ein, das Sie für RSA Security Analytics für den Zugriff auf Dateien auf dem Security Analytics Incident Management Integration Service-System erstellt haben.
9. Definieren Sie das Wiederholungsintervall für den Feed.
10. Definieren Sie im Bereich „Datumsbereich“ ein Start- und Enddatum für den Feed und klicken Sie auf **Weiter**.
11. Wählen Sie alle Decoder aus, auf die dieser Feed per Push übertragen werden soll, und klicken Sie auf **Weiter**.
12. Vergewissern Sie sich, dass im Feld „Typ“ die Option „IP“ ausgewählt ist.
13. Wählen Sie im Feld „Indexspalte“ den Wert „1“ aus.
14. Legen Sie in der zweiten Spalte für den Wert „Schlüssel“ das Wirksamkeitsrating fest und klicken Sie auf **Weiter**.
15. Überprüfen Sie die Details der Feedkonfiguration und klicken Sie auf **Fertigstellen**.

Managen des RSA Unified Collector Framework

Dieses Thema bietet zusätzliche Aufgaben für Konfiguration und Management der Integration von RSA UCF (Unified Collector Framework) für Archer SecOps 1.3.

Starten des RSA Unified Collector Framework

1. Klicken Sie auf **Systemsteuerung > Verwaltungstools > Services**.
2. Wählen Sie RSA Unified Collector Framework aus.
3. Klicken Sie auf **Start**.

Beenden des RSA Unified Collector Framework

1. Klicken Sie auf **Systemsteuerung > Verwaltungstools > Services**.
2. Beenden Sie den RSA SecOps-Watchdog-Service.

   Hinweis: Wenn Sie den Watchdog-Service nicht beenden, startet der Watchdog-Service den Security Analytics Incident Management Service frühzeitig.
3. Wählen Sie RSA Unified Collector Framework aus.
4. Klicken Sie auf **Stop**.

Hinweis: Wenn das Herunterfahren des Services zu lange dauert, verwenden Sie den Task-Manager, um den Prozess RSASAIMDCService zu beenden.

Deinstallieren des RSA Unified Collector Framework

1. Klicken Sie auf **Systemsteuerung** > **Programme und Funktionen**.
2. Wählen Sie **RSA Unified Collector Framework** aus.
3. Klicken Sie auf **Deinstallieren**.

Troubleshooting einer RSA Archer-Integration

Dieser Abschnitt enthält Lösungen für häufige Probleme, die bei der Konfiguration von Archer SecOps 1.2 oder Archer SecOps 1.3 mit Security Analytics Incident Management auftreten können.

Festlegen des Zertifizierungsstellen-Truststore

Problem: Nach dem Hinzufügen des Endpunkts für Security Analytics Incident Management kann der Zertifizierungsstellen-Truststore nicht festgelegt werden.

Lösung:

1. Vergewissern Sie sich, dass die SSH-Anmeldedaten für den Security Analytics-Host gültig sind.
2. Wenn die Anmeldedaten korrekt sind, der Fehler aber weiterhin auftritt, kopieren Sie die Zertifikate manuell.

Manuelles Kopieren von Enterprise-Management-Zertifikaten

Wenn Zertifikate nicht automatisch kopiert wurden, können Sie diese manuell kopieren.

1. Kopieren Sie das Zertifikat keystore-em.crt auf dem UCF-Computer von dem Speicherort: <install_dir>\SA IM integration service\cert-tool\certs auf den Security Analytics-Server unter /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.31-1.b13.el6_6.x86_64/jre/lib/security.
2. Melden Sie sich bei dem Computer an, auf dem RSA Security Analytics installiert wurde.
3. Navigieren Sie zu dem Speicherort, an dem sich das kopierte SA-Truststore-Zertifikat befindet:
   ```
   cd /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.31-1.b13.el6_6.x86_64/jre/lib/security
   ```
4. Führen Sie den folgenden Befehl aus:
   ```
   keytool -import -alias ucfcert -keystore cacerts -filekeystore-em.crt.der
   ```

Hinweis: Wenn Sie die Zertifikate kopiert haben, weil das Hinzufügen des Enterprise Management-Endpunkts fehlgeschlagen ist, müssen Sie den Endpunkt erneut hinzufügen, ohne die Zertifikate automatisch zu kopieren. Siehe **Konfigurieren von Endpunkten in RSA Unified Collector Framework** in Konfigurieren von Security Analytics für das Arbeiten mit Archer.

Security Analytics Incident Management-Zertifikate

Wenn Zertifikate nicht automatisch kopiert werden, können Sie diese manuell kopieren.

1. Kopieren Sie das Zertifikat keystore.crt.pem von <install_dir>\SA IM integration service\cert-tool\certs auf dem UCF-Computer nach Pfad/tmp auf dem Security Analytics-Server.
2. Melden Sie sich bei dem Computer an, auf dem RSA Security Analytics installiert wurde.
3. Navigieren Sie zu /tmp.
4. Geben Sie Folgendes ein, um das UCF-Zertifikat an Security Analytics RabbitMQ anzuhängen:
   ```
   cat keystore.crt.pem >>
   /etc/puppet/modules/rabbitmq/files/truststore.pem
   ```
5. Geben Sie Folgendes ein:
   ```
   >puppet agent -t
   ```
6. Sobald der Agent abgeschlossen ist, beenden Sie den Verbindungsmanager.
7. Starten Sie den RSA Unified Collector Framework-Service von services.msc neu.
8. Führen Sie den Verbindungsmanager erneut aus, um mit der Konfiguration der SA-Endpunkte fortzufahren.

Incidents in der RSA Archer Security Operations Management-Lösung

Problem: Befunde und Sicherheits-Incidents werden nicht in der RSA Archer Security Operations Management-Lösung angezeigt.

Lösung:

1. Vergewissern Sie sich, dass die Uhrzeit auf dem Middleware-System und der RSA Archer-Plattform synchronisiert oder der Unterschied nicht größer als eine Sekunde ist.
2. Überprüfen Sie, ob der Endpunkt korrekt konfiguriert ist.
3. Vergewissern Sie sich, dass für das UCF der korrekte Modus festgelegt ist.
   - Für Befunde sollten Sie auswählen, dass der Incident-Workflow in RSA Security Analytics gemanagt wird.
   - Für Sicherheits-Incidents sollten Sie auswählen, dass der die Incident-Workflow in RSA Archer Security Operations Management gemanagt wird.

4. Stellen Sie über SSH eine Verbindung zum SA-Webserverhost her und geben Sie den folgenden Befehl ein, um zu überprüfen, ob die RSA Archer-Incident-Warteschlange (im.archer_incident_queue) erstellt wird:

```
curl -k -u guest:guest
https://127.0.0.1:15671/api/queues/%2Frsa%2Fi
m%2Fintegration/im.archer_incident_queue --
silent --stderr - | grep -o '"name"\:.*
```

Hinweis: Wenn die Warteschlange erstellt wird, lautet die Ausgabe wie folgt:

```
"name":"im.archer_incident_
queue","vhost":"/rsa/im/integration","durable
":true,"auto_delete":false,"arguments":
{},"node":"sa@localhost"}
```

5. Stellen Sie über SSH eine Verbindung zum SA-Webserverhost her und geben Sie den folgenden Befehl ein, um zu überprüfen, ob die RSA Archer-Ticket-Warteschlange (im.archer_tickets_queue) erstellt wird:

```
curl -k -u guest:guest
https://127.0.0.1:15671/api/queues/%2Frsa%2Fi
m%2Fintegration/im.archer_tickets_queue --
silent --stderr - | grep -o '"name"\:.*'
```

Hinweis: Wenn die Warteschlange erstellt wird, lautet die Ausgabe wie folgt:

```
"name":"im.archer_tickets_
queue","vhost":"/rsa/im/integration","durable
":true,"auto_delete":false,"arguments":
{},"node":"sa@localhost"}
```

6. Stellen Sie über SSH eine Verbindung zum SA-Webserverhost her und geben Sie den folgenden Befehl ein, um die Anzahl der Meldungen in der Incident-Warteschlange zu überprüfen:

```
curl -k -u guest:guest
https://127.0.0.1:15671/api/queues/%2Frsa%2Fi
m%2Fintegration/im.archer_incident_queue -- silent --stderr -
| grep -o '"messages"\:[0-
9]*'
```

Hinweis: Wenn die Warteschlange erstellt wird, lautet die Ausgabe wie folgt:
`"messages" : 5`

7. Vergewissern Sie sich, dass die oben genannten Warteschlangen mit Meldungen des UCF gefüllt werden.

Korrekturaufgaben in RSA Archer Security Operations Management

Problem: Korrekturaufgaben werden per Push über den UCF in die Vorgangswarteschlange übertragen und nicht als Befunde in RSA Archer Security Operations Management angezeigt.

Lösung:

1. Öffnen Sie den Verbindungsmanager:
   - Öffnen Sie eine Eingabeaufforderung
   - Wechseln Sie zum Verzeichnis <install_dir>\SA IM integration service\data-collector.
   - Geben Sie Folgendes ein: runConnectionManager.bat
2. Geben Sie „2“ für „Endpunkt bearbeiten“ ein.
3. Geben Sie „3“ für Security Analytics Incident Management ein.
4. Vergewissern Sie sich, dass die Zielwarteschlange auf „Alle“ oder „Vorgänge“ festgelegt ist.

Fehler zwischen RSA Security Analytics und RSA Unified Collector Framework

Problem: In <*install_dir*>\SA IM integration service\logs\collector.log sind SSL-Fehler zwischen RSA Security Analytics und RSA Unified Collector Framework protokolliert.

Lösung:

1. Vergewissern Sie sich, dass die SSL-Zertifikate gültig sind.

   Hinweis: Security Analytics Incident Management-Zertifikate sind zwei Jahre lang gültig.

2. Wenn die Zertifikate abgelaufen sind, erzeugen Sie die abgelaufenen Zertifikate erneut und kopieren Sie diese.

Gehen Sie wie folgt vor, um die Zertifikate neu zu erzeugen und zu kopieren:

1. Navigieren Sie in der Eingabeaufforderung zu <*install_dir*>\SA IM integration service\data-collector.

2. Geben Sie Folgendes ein: `runConnectionManager.bat`
3. Geben Sie die Zahl für „Security Analytics Incident Management Integration Service-Zertifikat neu erzeugen“ ein.
4. Geben Sie im Verbindungsmanager im Security Analytics Incident Management-Endpunkt die Zahl für „Endpunkt bearbeiten“ ein.
5. Geben Sie „Ja“ ein, um die Zertifikate automatisch in den Security Analytics-Truststore zu kopieren.

Hinweis: Wenn die Zertifikate nicht kopiert werden, kopieren Sie diese manuell.